REMARKS

The present response is intended to be fully responsive to the rejection raised in the Office action, and is believed to place the application in condition for allowance. Further, the Applicant does not acquiesce to any portion of the Office Action not particularly addressed. Favorable reconsideration and allowance of the application is respectfully requested.

In the Office action, the Office noted that claims 1-16 are pending and rejected. Applicant amends claims 1 and 13. Applicant has not introduced any new matter by way of the foregoing amendments.

In view of the above amendments and the following discussion, the Applicant submits that none of the claims now pending in the application are anticipated under the provisions of 35 U.S.C. § 102 or obvious under the provisions of 35 U.S.C. § 103. Thus, Applicant believes that all of these claims are now in condition for allowance.

OBJECTION

The Office objected to claims 1 and 13 for lacking antecedent basis for the term "the determinant". Applicant thanks the Office for pointing the anomaly and amends claims 1 and 13 to remedy it. More specifically, Applicant amends claims 1 and 13 to recite "a determinant", thus, providing proper antecedent basis. Therefore, Applicant requests reconsideration and withdrawal of the objection to claims 1 and 13.

REJECTION

The Office rejected claims 9-12 and 15-16 under 35 U.S.C. § 102(e) as being unpatentable over U.S. Patent Publication No. 2003/0028484 published to Boylan et al. (Hereon after "*Boylan*"). Moreover, the Office rejected claims 13 and 14 under 35 U.S.C. § 102(e) as being unpatentable over U.S. Patent No. 6,901,145 issued to Bohannon et al. (Hereon after "*Bohannon*"). In addition, the Office rejected claims 1-8 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,901,145 issued to Bohannon et al. (Hereon after "*Bohannon*") in view of U.S. Patent

Publication No. 2004/0062390 published to Slavin et al. (Hereon after "*Slavin*"). The Applicant respectfully traverses the rejections.

A. Applicant's Response to the 35 U.S.C. § 102(e) Rejection of claims 9-12 and 15-16

The Office rejected claims 9-12 and 15-16 under 35 U.S.C. § 102(e) as being unpatentable over *Boylan*. The Applicant traverses the rejection.

As the Examiner is aware, "anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Maschinen Fabrick GmbH v. American Hoist Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984) [emphasis added]. Applicant submits that the cited reference is devoid from disclosing at least one element recited in Applicant recited invention.

In the Office Action, the Office insinuated that *Boylan* discloses all the elements recited in claim 9. In support of the rejection, the Office indicated that Boylan discloses "encrypting said processed message with block-based encryption method which has blocks smaller than said preprocessed message ([0008], lines 20-21)." Office Action, at page 3. Applicant respectfully disagrees.

Claim 9 recites a combination of elements directed to a method of encryption. The combination of elements includes defining a permutation source; generating a permuted message for an input message employing said permutation source; padding said permuted message with said permutation source to obtain a preprocessed message; and encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message. [Emphasis Added]

Boylan, on the other hand, discloses a method of inter-terminal payment and corresponding devices and computer programs loadable into said devices. *Boylan,* at Abstract. *Boylan* discloses an electronic context signature is established in detail by first hashing the message via 160-bit cryptographic hash function… followed by a padding of the hash value… and finally building a retail Cipher Block Chaining Message Authentication Code (CBC-MAC) according to American National Standards Institute (ANSI) X9.19 standard using the 2-Ke-Triple DES encryption method." *Boylan*, paragraph [0008], lines 14-21.

Therefore, *Boylan* discloses hashing a message via cryptographic hash function, padding the hash value and building retail Cipher Block Chaining according to ANSI. Therefore, unlike claim 1, *Boylan* is devoid from suggesting or disclosing "encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message," as recited in claim 9. Thus, Applicant submits that *Boylan* does not teach all the elements recited in claim 9. The Applicant submits that *Boylan* does not anticipate claim 9. Hence, claim 9, in view of *Boylan,* satisfies the requirements of 35 U.S.C. § 102(e) and is in condition for allowance.

Claims 10-12 and 15-16 depend, directly or indirectly, from claim 9 and, thus, necessarily contain each and every element recited in claim 9. Since the Applicant submits that *Boylan* does not anticipate claim 9, the Applicant further submits that *Boylan* also does not anticipate claims 10-12 and 15-16. Hence, claims 9-12 and 15-16 satisfy the requirements of 35 U.S.C. § 102(e) and are in condition for allowance.

B. **Applicant's Response to the 35 U.S.C. § 102(e) Rejection of claims 13 and 14**

The Office rejected claims 13 and 14 under 35 U.S.C. § 102(e) as being unpatentable over *Bohannon*. The Applicant traverses the rejection.

As the Examiner is aware, "anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Maschinen Fabrick GmbH v. American Hoist Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984) [emphasis added]. Applicant submits that the cited reference is devoid from disclosing at least one element recited in Applicant recited invention.

Amended claim 13 recites a combination of elements directed to a method of decrypting. The combination of elements includes "computing a determinant of a matrix-based encrypted message matrix, wherein said encrypted message was generated by partitioning an input message into matrix elements…."

The Office indicated that *Bohannon* "doesn't explicitly disclose…partitioning an input message into matrix elements." *Office Action*, at page 4. Applicant agrees with the Office. Therefore, *Bohannon* does not disclose all the elements recited in

amended claim 13. Consequently, the Applicant submits that *Bohannon* does not teach all the elements recited in claim 13. The Applicant submits that *Bohannon* does not anticipate claim 13. Hence, claim 13, in view of *Bohannon,* satisfies the requirements of 35 U.S.C. § 102(e) and is in condition for allowance.

Claim 14 depends directly from amended, independent claim 13 and necessarily contains each and every element recited in their respective claim. Since the Applicant submits that *Bohannon* does not anticipate claim 13, the Applicant further submits that *Bohannon* also does not anticipate claim 14. Hence, claims 13 and 14 satisfy the requirements of 35 U.S.C. § 102(e) and are in condition for allowance.

C. Applicant's Response to the 35 U.S.C. § 103(a) Rejection of claims 1-8

The Office rejected claims 1-8 under 35 U.S.C. § 103(a) as being unpatentable over *Bohannon* in view of *Slavin*. In support of the rejection, the Office indicated that *Bohannon* "doesn't explicitly disclose…partitioning an input message into matrix elements… *Salavin* discloses (a) partitioning an input message into matrix elements ([0055], see also [0033], [0044])." The Applicant agrees that *Bohannon* doesn't explicitly disclose partitioning an input message into matrix elements and respectfully traverses the rejection.

As the Examiner is aware, to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claimed limitations. The teaching or suggestions to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F. 2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Furthermore, as the Office is also aware, the courts have repeatedly stated that a prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. V. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983).

Bohannon discloses a repeatable cryptographic key, which is "generated based on varying parameters which represent physical measurements," wherein "the secret key k is computed as the determinant of am mxm matrix over the integers mod q." *Bohannon*, at Abstract and col. 10 lines 64-67. Furthermore, *Bohannon* discloses cryptographic shares that "are used to compose the matrix." *Id*. *Bohannon* specifically teaches:

> "To provide context-less servers with public-key encryption, it is desirable not to keep client-specific private symmetric-keys on the server. In this case, the slow decryption rate of public keys can be a problem, even when they are used only to exchange a secret key. Further, the processing requirements for performing simultaneous encryption and decryption should be reduced, allowing for use in low-power applications, such as cell phones, or web-based radio communication systems, such as, blue-tooth and wireless LAN." *Id.* at ¶[0014], also look at [0007]-[0015].

Slavin, on the other hand, "provides a technique for secure messages transmission using a public key system to exchange secret keys." *Slavin* also discloses "a symmetric-key encryption algorithm includes partitioning and packaging an obtained message into a sequence of unencrypted matrices Ui." *Id.* at ¶[0055].

Accordingly, it is Applicant's opinion that *Bohannon* teaches away from the teaching of *Slavin*. *Bohannon* and *Slavin*, alone and in combination, do not suggest or show a motivation for modifying the reference or to combine the reference teachings. In addition, it is Applicant's opinion that there is no evidence in any of the prior art that shows a "reasonable expectation of success" in combining the references. Thus, it is Applicant's belief that a prima facie case of obviousness has not been provided. The Applicant submits that *Bohannon* and *Slavin*, alone and in combination, do not disclose all the elements or render claim 1 obvious

Given that each of the dependent claims 2-8 depend, directly or indirectly, from independent claim 1, each necessarily includes all the elements of claim 1. Since Applicant submits that *Bohannon* and *Slavin*, alone and in combination, do not disclose all the elements or render claim 1 obvious, the Applicant further submits that *Bohannon* and *Slavin,* alone and in combination, also do not disclose all the elements or render claims 2-8 obvious. The Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 1-8.

CONCLUSION

In view of the foregoing, the Applicant submits that none of the claims presently in the application are anticipates under 35 U.S.C. §102 or obvious under the provisions of 35 U.S.C. §103. Consequently, the Applicant believes that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Office believes that any unresolved issues still exist or if, in the opinion of the Office, a telephone conference would expedite passing the present application to issue, the Office is invited to call the undersigned attorney directly at 972-917-4365 or the office of the undersigned attorney at 972-917-4363 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

Date: May 1, 2008

By: /Mirna Abyad/
MIRNA ABYAD
Registration No. 58,615
Texas Instruments
P.O. Box 655474, M/S 3999
Dallas, TX 75265
Telephone: (972) 917-4365